



Sécurité bureautique avec les produits de certification ASIP Santé (carte CPS et certificats logiciels)

Sécurité bureautique avec les produits de certification ASIP Santé (carte CPS et certificats logiciels)

Version 2.0.1 du 30/09/2015

Historique du document

Version	Date	Auteur	Commentaires
1.00	01/08/2011	ASIP Santé	Création (Outlook et chiffrement)
1.20	03/08/2011	ASIP Santé	Outlook et signature
2.0.0	14/09/2015	ASIP Santé	Adobe et signature
2.0.1	30/09/2015	ASIP Santé	PFCNG

1 Références

N°	Version	Date	Auteur	Document
[1]	5.1.2	09/07/2015	ASIP Santé	Manuel d'installation et d'utilisation de la Cryptolib CPS v5
[2]	2.1	18/03/2015	GIE SESAM-Vitale	Manuel d'installation du GALSS

Tableau 1 : Références

2 Résumé

La carte CPx distribuée par l'ASIP Santé contient un certificat de signature. Ce certificat est exposé auprès des systèmes d'exploitation au moyen de la Cryptolib CPS v5, ce qui permet d'effectuer des opérations de signature de documents depuis les applications de bureautique usuelles (Microsoft Word, Microsoft Outlook, Adobe Acrobat Reader) avec la carte CPx.

La carte CPx permet aussi de commander un bi-clé de confidentialité avec l'outil CleoCPS. Le certificat associé peut être diffusé à des « tiers correspondants » pour qu'ils chiffrent leurs messages (emails, fichiers) à destination du détenteur du certificat qui sera le seul à pouvoir les déchiffrer.

Le présent document décrit comment mettre en œuvre de telles fonctionnalités.



Accompagnement

Pour toute question et échange sur ce document :

editeurs@asipsante.fr

Tableau 2 : contact accompagnement ASIP Santé

3 Sommaire

1	Références	3
2	Résumé	3
3	Sommaire	4
4	Glossaire	5
5	Liste des entreprises citées	6
6	Avertissements	7
7	Microsoft Outlook	8
7.1	Produits concernés	8
7.1	Prérequis	8
7.2	Rappels d'architecture	9
7.2.1	Configuration nominale « lecteurs PC/SC »	9
7.2.2	Configuration nominale « lecteurs PSS »	10
7.3	Signature de messages électroniques	11
7.3.1	Configurer Microsoft Outlook pour accepter de signer avec les cartes CPS	11
7.3.2	Signature d'un email	13
7.3.1	Réception d'un email signé	14
7.4	Déchiffrement de messages électroniques avec Outlook	17
7.4.1	Rappels	17
7.4.1	Commander un certificat de confidentialité avec la carte CPS	18
7.4.2	Configurer Microsoft Outlook pour déchiffrer des emails	18
7.5	Chiffrement de messages électroniques	19
8	Adobe Acrobat Reader	20
8.1	Signature de PDF avec Adobe Acrobat Reader	20
8.2	Vérification de signature avec Adobe Acrobat Reader	24
8.2.1	Configuration	24
8.2.2	Vérification de signature	24
8.3	Utilisation du PKCS#11	26
8.4	Déploiement de Adobe Acrobat Reader en entreprise	29
8.5	Création automatisée de documents PDF signés	29
9	Conseils et Performances	30
9.1	Commande de produits de certification	30
9.2	Provider de révocation ASIP Santé / Microsoft (PRAM)	30
9.3	Récupération des CRLs ASIP Santé	30
9.4	Sécurisation de mails « point à point » versus MSSanté	31
9.5	Calcul du Hash	31
10	Annexe – Liste des figures	32
11	Annexe – Liste des tableaux	32
12	Notes	33

4 Glossaire

Abréviation	Signification
ASIP Santé	Agence des Systèmes d'Information Partagés de Santé
CPx	Famille de cartes à puce émises par l'ASIP Santé comprenant CDA, CDE, CPA, CPE, CPF et CPS
FS	File System – Système de fichiers
GALSS	Gestionnaire d'Accès aux Lecteurs Santé Social
GIE	Groupement d'Intérêt Economique
OS	Operating System – Système d'exploitation
PC/SC	Personal Computer / Smart Card
PFCNG	Plate-Forme de Certification Nouvelle Génération
PSS	Protocole Santé Social

Tableau 3 : Glossaire

5 Liste des entreprises citées

Le présent document cite les produits des entreprises ou organismes suivants:

Nom	Site Web	Lien avec le document
Adobe	www.adobe.com	Editeur de Acrobat Reader
ASIP Santé	www.sante.gouv.fr	CPx, Cryptolib CPS v5, testssl.asipsante.fr, DMP, MSSanté
Microsoft	www.microsoft.com	Editeur du système d'exploitation Windows et de la suite Office (Outlook, Word, Excel)

Tableau 4 : Entreprises citées

6 Avertissements

Sur le nécessaire strict respect des procédures décrites dans le document

L'attention de l'utilisateur est attirée sur l'importance de respecter strictement les procédures décrites dans le présent document.

Toutes les procédures qui y sont décrites ont été préalablement testées par l'ASIP Santé. En cas de non-respect de ces procédures, des dysfonctionnements dans l'environnement de travail de l'utilisateur peuvent apparaître.

En cas de dysfonctionnement, quel qu'il soit, l'ASIP Santé prêtera dans la mesure du possible assistance à l'utilisateur, qui ne pourra rechercher sa responsabilité en cas de non-respect des procédures décrites dans le présent document.

Sur les liens externes

Le présent document contient des liens vers des sites Internet.

Ces liens ne visent qu'à informer l'utilisateur. Ces sites Web ne sont pas gérés par l'ASIP Santé et l'ASIP Santé n'exerce sur eux aucun contrôle : leur mention ne saurait engager l'ASIP Santé quant à leur contenu.

L'utilisation des sites tiers mentionnés relève de la seule responsabilité du lecteur ou de l'utilisateur des produits documentés.

Sur les copies d'écran

Les copies d'écran présentées dans ce document sont données à titre illustratif.

Les pages ou écrans réellement affichés peuvent être différents, notamment en raison de montées de version ou de configurations d'environnements différentes.

Citations

L'ASIP Santé est contrainte de citer le nom de certaines entreprises recensées au Tableau 4 afin d'apporter toute l'aide nécessaire au lecteur.

Les entreprises citées peuvent prendre contact avec l'ASIP Santé à l'adresse email editeurs@asipsante.fr pour toute demande en lien avec la citation les concernant.

Les entreprises non citées dans ce manuel et ayant une activité en lien avec la carte CPx ou les IGC peuvent également se faire connaître auprès de l'ASIP Santé en la contactant à la même adresse.

Tableau 5 : Avertissements

7 Microsoft Outlook

7.1 Produits concernés

Les versions de Microsoft Outlook concernées sont :

- Microsoft Outlook 2000
- Microsoft Outlook 2002
- Microsoft Outlook 2003
- Microsoft Outlook 2007
- Microsoft Outlook 2010
- Microsoft Outlook 2013

7.1 Prérequis

#	Prérequis
1	Posséder une carte CPS non bloquée, non expirée, non opposée, en bon état
2	Posséder un lecteur de carte CPS (lecteur PSS avec un firmware à jour ou lecteur PC/SC)
3	Avoir installé la Cryptolib CPS v5 sur le poste
4	Faire confiance aux autorités intermédiaires et racines correspondant aux certificats CPS (mise à jour de magasins de certificats, normalement faite par la Cryptolib CPS v5)
5	Posséder une licence Microsoft Windows et Microsoft Outlook

Tableau 6 : Prérequis

7.2 Rappels d'architecture

7.2.1 Configuration nominale « lecteurs PC/SC »

Avec la Cryptolib CPS v5 et un lecteur PC/SC, l'architecture logicielle mise en œuvre pour accéder à la CPx lors d'une signature d'email par Microsoft Outlook est la suivante :

Légende

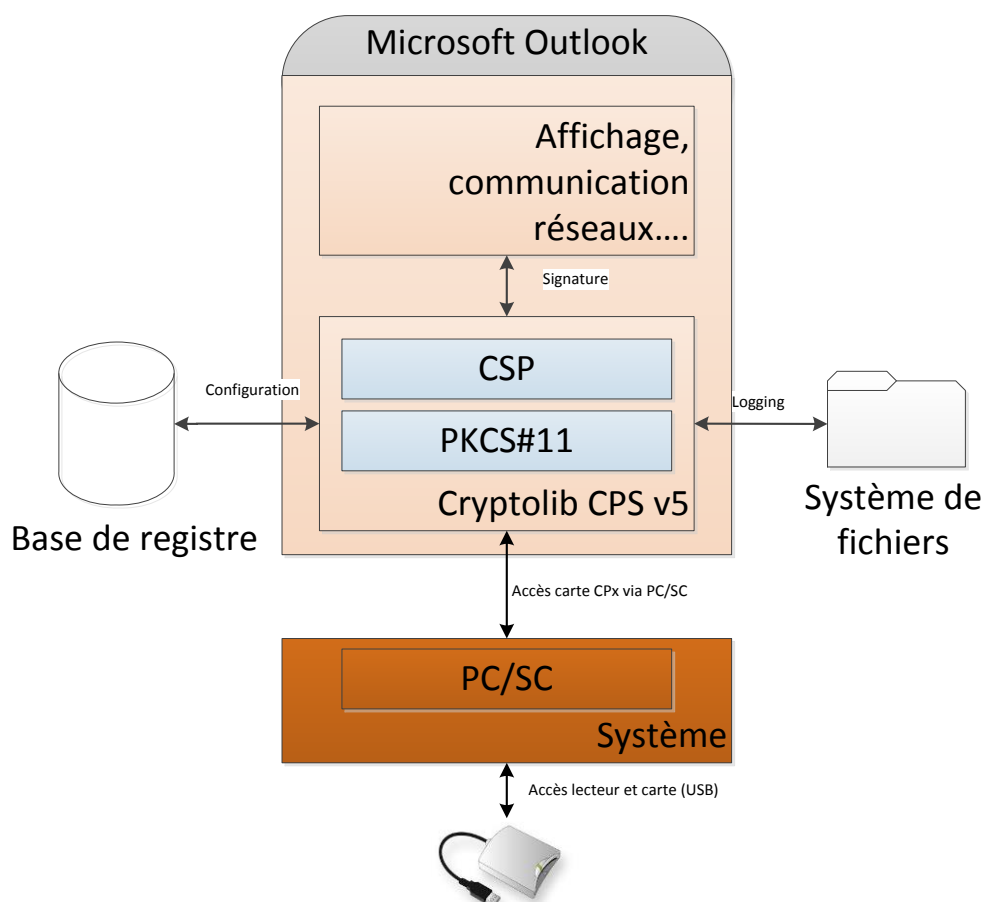


Figure 1 : Architecture d'accès à la CPS avec Outlook en configuration PC/SC

7.2.2 Configuration nominale « lecteurs PSS »

Sous Windows, le GALSS est installé par un installeur (.msi).

L'installateur installe les 2 parties qui composent le GALSS :

- 1- Un « serveur », unique et instancié sous le compte de l'utilisateur, qui prend la forme d'un exécutable (galsvw32.exe généralement) et qui gère les communications vers les lecteurs au gré des demandes de applications
- 2- Des « clients », instanciés par chaque application opérant avec des cartes et communiquant avec l'unique serveur via des « Named pipe »

L'architecture générale est la suivante :

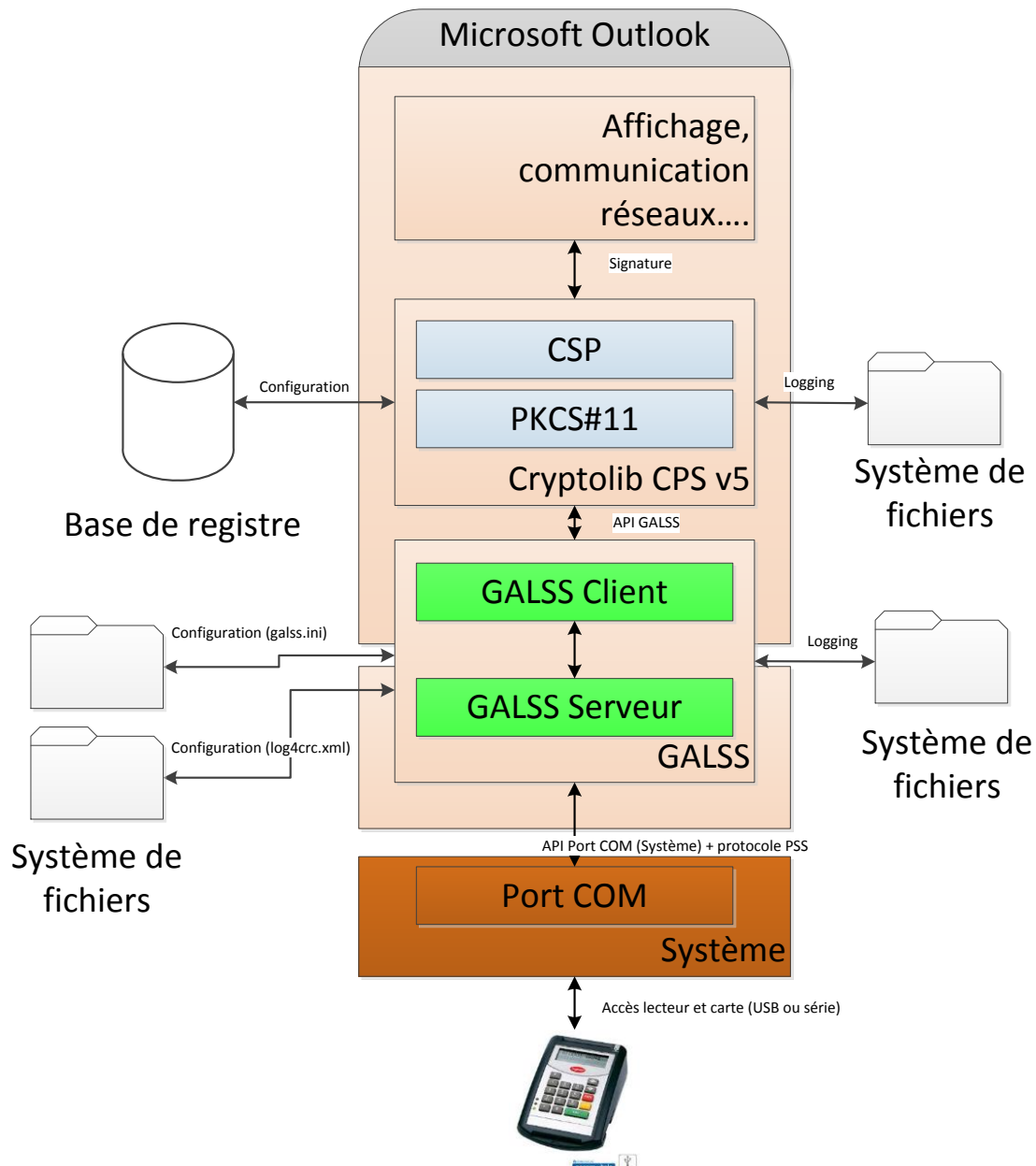


Figure 2 : Architecture d'accès à la CPS avec Outlook en configuration PSS

7.3 Signature de messages électroniques

7.3.1 Configurer Microsoft Outlook pour accepter de signer avec les cartes CPS

Le certificat de signature de la carte CPS n'a pas d'adresse e-mail. Pour qu'Outlook puisse l'utiliser pour signer des emails, il faut désactiver le contrôle qu'il effectue sur ce champ via la base de registres en ajoutant une clé à l'endroit suivant.

Version	Clé
Outlook 2013	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\15.0\Outlook\Security
Outlook 2010	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\14.0\Outlook\Security
Outlook 2007	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\12.0\Outlook\Security
Outlook 2003	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\11.0\Outlook\Security
Outlook 2002	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\10.0\Outlook\Security
Outlook 2000	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Office\9.0\Outlook\Security



clé « Security »

Si la clé « Security » n'existe pas, il est nécessaire de la créer

Tableau 7 : Clé Security absente



Signature CPS avec Outlook et PFCNG

La nouvelle IGC de Santé (PFCNG) permet de passer commande de certificats logiciels de personnes physiques ou de certificats cartes contenant des adresses mail, ce qui permet d'éviter cette désactivation.

Tableau 8 : Signature CPS avec Outlook et PFCNG

clé	Type	Valeur
SupressNameChecks »	dword	1



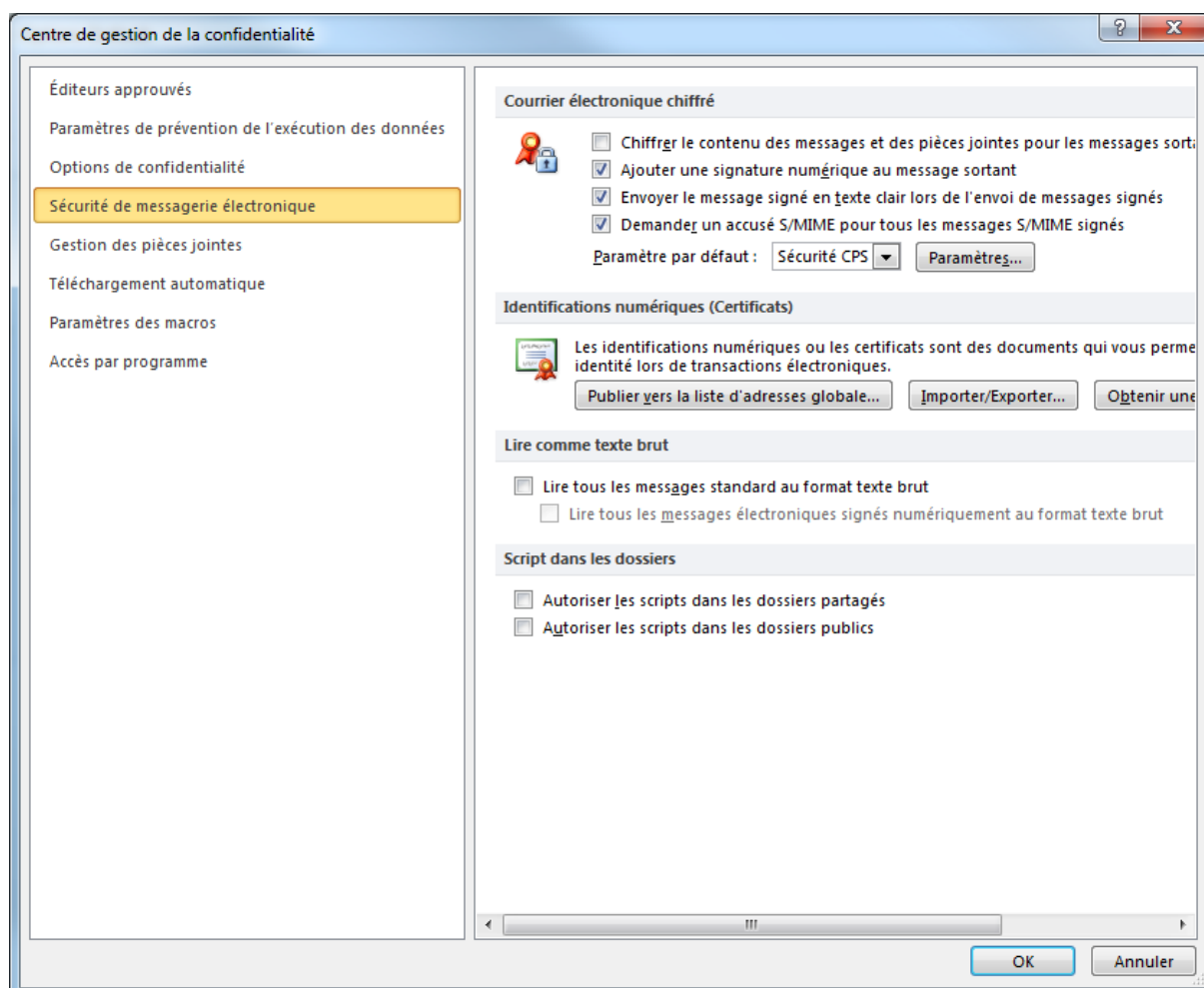
Redémarrage

Redémarrer Microsoft Outlook pour que ce paramétrage soit pris en compte.

Tableau 9 : Redémarrage d'Outlook

#	Configurer Outlook pour utiliser le certificat de signature de la carte CPS
1	Menu "Outils" => "Centre de gestion de confidentialité" => "sécurité de messagerie électronique" => "Paramètres" => "Nouveau" Menu "Fichiers"=> "Options" => "Centre de gestion de confidentialité" => "Paramètres du Centre de gestion de la confidentialité..." => "Sécurité de messagerie électronique" => "Paramètres" => "Nouveau"
2	Saisir un nom de paramètre de sécurité (par exemple « Sécurité CPS »)
3	Bouton "Choisir" (certificat de signature) => sélectionner le certificat de signature correspondant à la carte CPS insérée dans le lecteur
4	Choisir « SHA1 » pour l'algorithme de hachage
5	Refermer les fenêtres en validant les choix (« OK »)

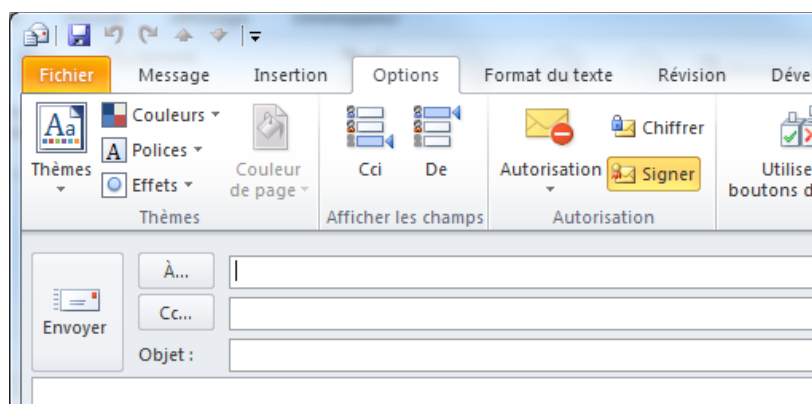
Afin de signer tous les emails sortant, cocher l'option « ajouter une signature numérique au message sortant » :



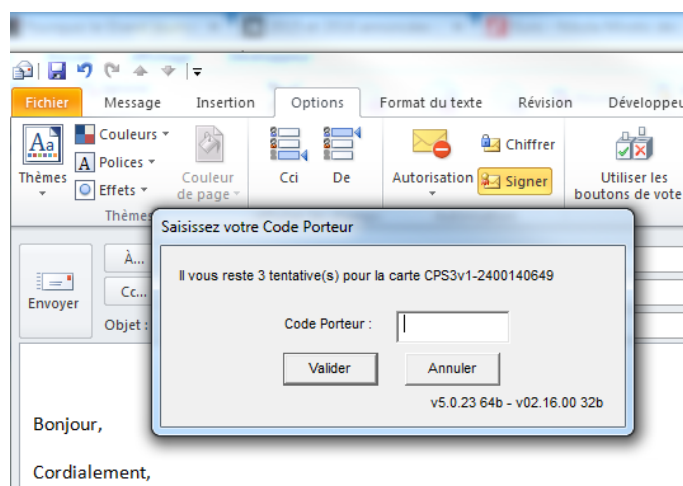
7.3.2 Signature d'un email

Rédiger un email comme à l'habitude ("Nouveau message électronique").

L'option de signature de l'email peut être activée ou désactivée en cochant/décochant la case « Signer » dans la barre de menu d'édition d'un nouvel email :



Lors de l'envoi de l'email, le code porteur de la carte CPS sera demandé pour signer le message :

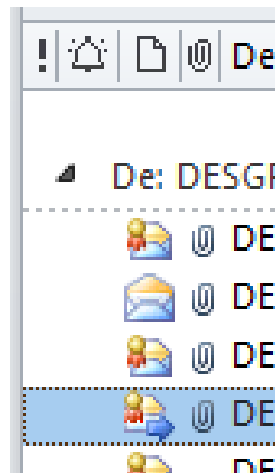


Une fois l'email signé envoyé, il apparaît dans les « Eléments envoyés » accompagné d'un icône représentant un sceau de signature :

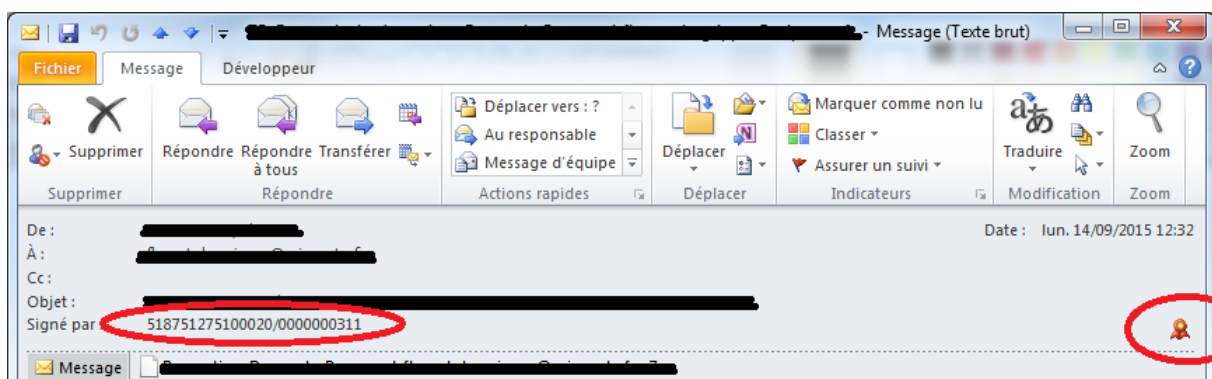


7.3.1 Réception d'un email signé

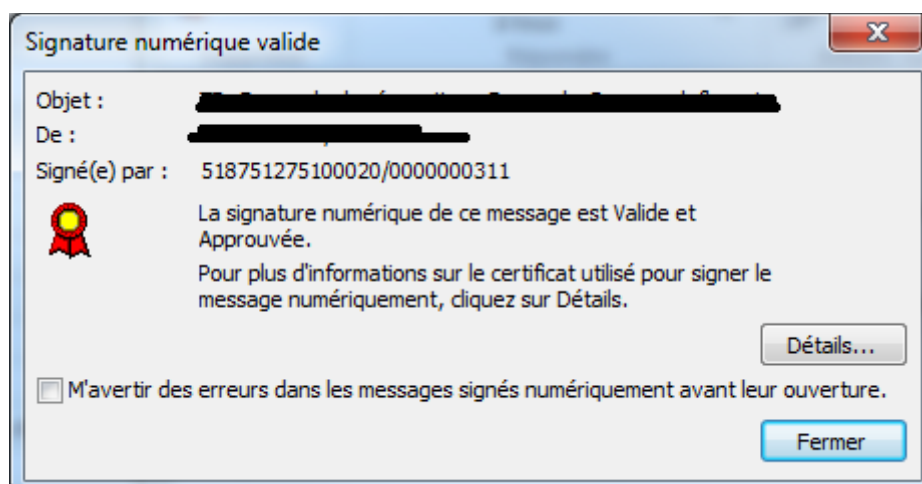
A la réception, un email signé apparaît lui aussi accompagné d'un icône représentant un sceau de signature :



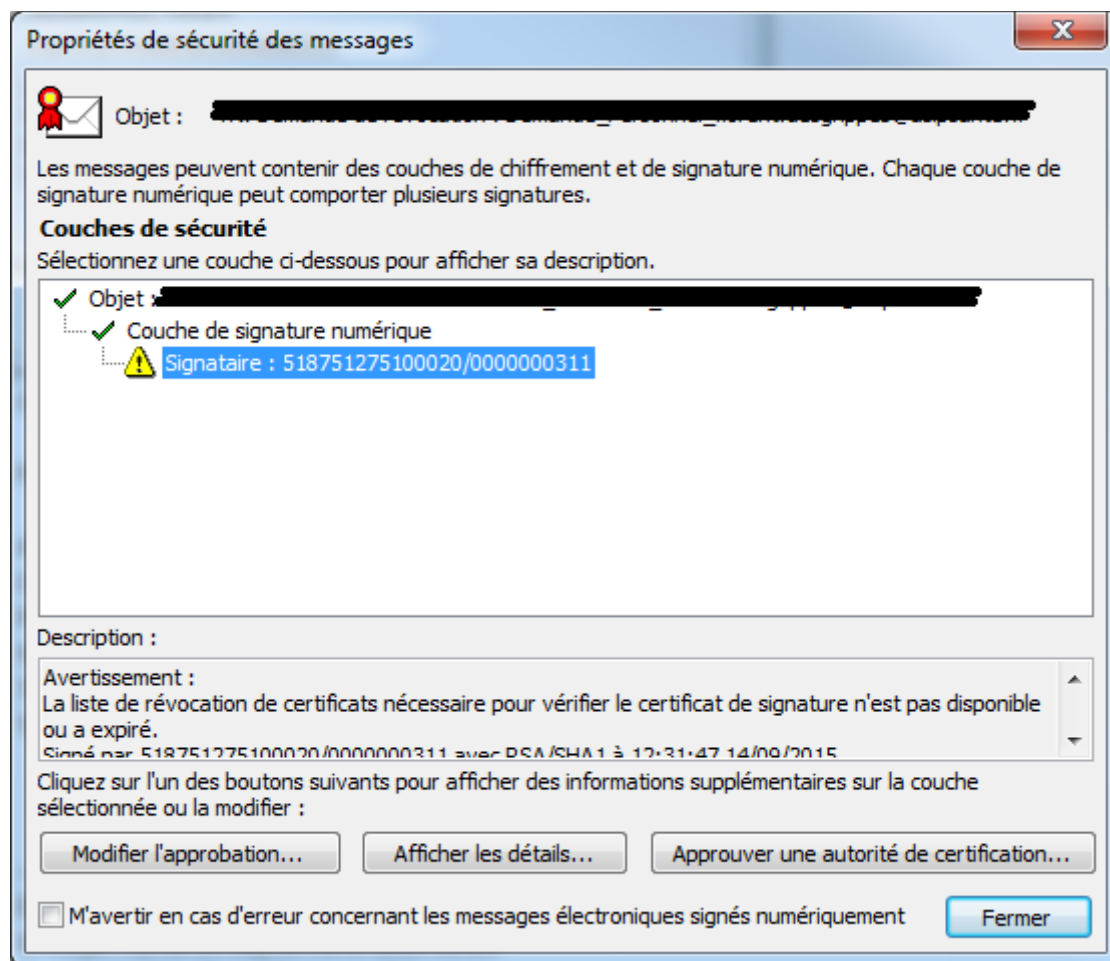
Lorsque qu'on ouvre l'email en question, Outlook signale que l'email est signé :



Un clic sur le sceau permet de faire apparaître la signature :



Un clic sur « Détails... » permet de faire apparaître le détail de la signature :



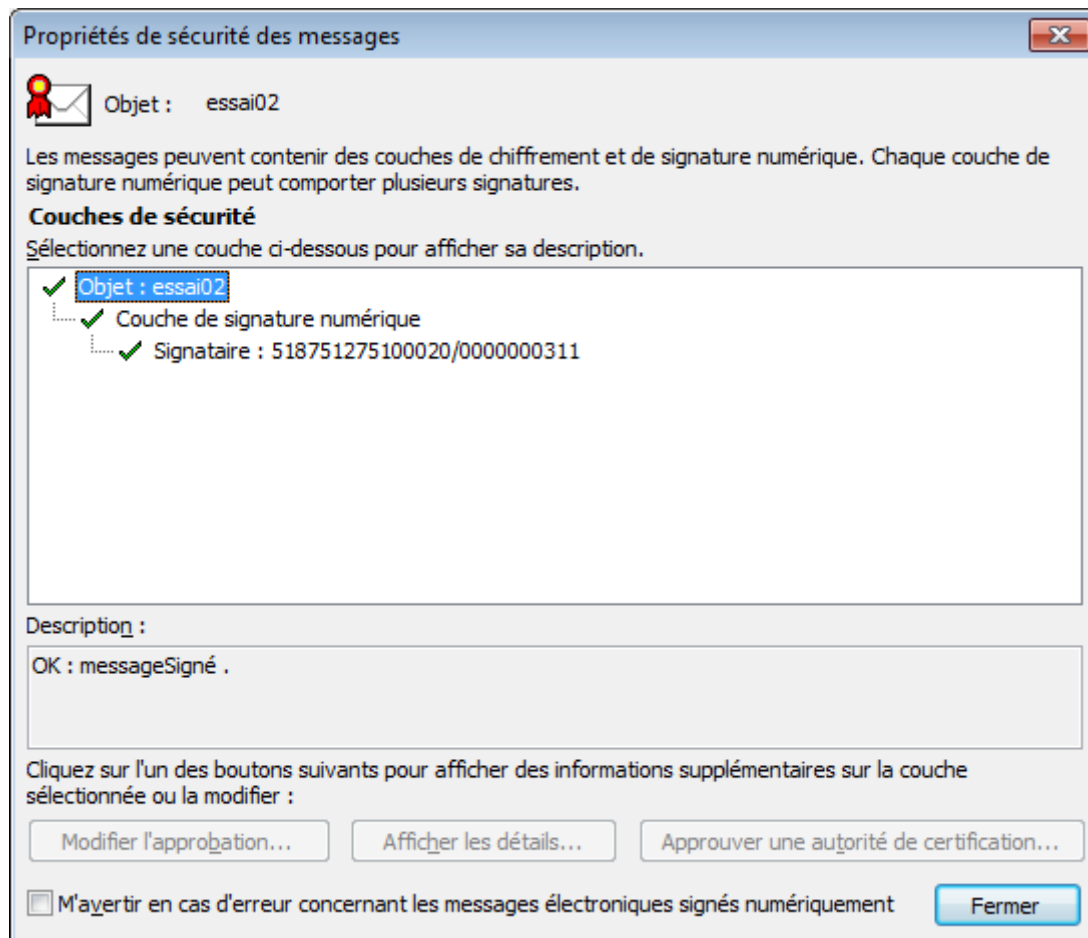
Le point d'exclamation est un avertissement. Il est dû à l'échec de la vérification de la signature de la CRL (liste de révocation) ASIP Santé : le statut du certificat n'a pas été vérifié complètement (vérification du statut de révocation manquante).

Ce problème est lié au fait que, dans l'IGC ASIP Santé, l'autorité de certification signe les certificats CPS avec un bi-clé et la CRL associées avec un autre bi-clé. Ce mode de signature est décrit dans la section § 5.1.1.3 du RFC 5280.

Le module natif de Windows de vérification des statuts de certificats (cryptnet.dll) ne supporte pourtant pas ce mode de signature : la vérification échoue.

Pour remédier à ce problème, il faut déclarer auprès du système un « provider de révocation » spécifique à l'IGC ASIP Santé, développé en partenariat avec Microsoft (« Provider de Révocation ASIP Santé / Microsoft » ou PRAM). Toutes les informations et le téléchargement de ce module se trouve à l'adresse suivante : <http://www.microsoft.com/france/interop/ressources/gip-cps.aspx>

Une fois le PRAM installé, la vérification de statuts passe à condition que les flux **HTTP (TCP port 80)** ou **LDAP (TCP port 389)** vers le domaine **annuaire.asipsante.fr** soient ouverts :



7.4 Déchiffrement de messages électroniques avec Outlook

7.4.1 Rappels

Le chiffrement d'un message électronique protège ce message en confidentialité : le texte brut, lisible est converti en texte chiffré.

Seul le destinataire disposant de la clé privée qui correspond à la clé publique que a été utilisée pour chiffrer le message peut déchiffrer celui-ci.

La carte CPS sert à générer un certificat de confidentialité associé à cette carte (certificat classe 5 émis par l'IGC de Santé 2Bis) :

- Le porteur CPS commande en certificat de confidentialité Classe 5 avec sa CPS et CleoCPS
- Le porteur garde la clé privée associée à ce certificat de confidentialité Classe 5 bien précieusement dans son magasin de bi-clé personnel Microsoft
- Ses interlocuteurs utilisent le certificat de confidentialité Classe 5 (clé publique + éléments d'identité + éléments de révocation) pour chiffrer leurs emails à destination du porteur CPS
 - Lors de cette phase de chiffrement de message, la carte CPS n'est bien sûr pas utilisée
 - Les interlocuteurs de porteur CPS ne portent pas la carte du porteur CPS en question !
 - C'est la clé publique contenue dans le certificat classe 5 qui est utilisée (information publique)
- Le porteur CPS utilise Microsoft Outlook pour relever les emails qui lui sont adressés chiffrés par ses interlocuteurs et la clé privée associée à ce certificat de confidentialité Classe 5 stockée en magasin pour déchiffrer les messages reçus
 - Lors de cette phase de déchiffrement de message, la carte CPS n'est pas utilisée
 - C'est la clé privée correspondant au classe 5 qui est utilisée (bi-clé logiciel)

7.4.1 Commander un certificat de confidentialité avec la carte CPS

#	Commander un certificat de confidentialité avec la carte CPS
1	Obtenir un certificat de chiffrement personnel auprès de l'autorité d'enregistrement de l'ASIP Santé correspondant à votre carte CPS.
	Utiliser CleoCPS, un utilitaire d'aide à la génération de certificat de chiffrement (appelé certificat personnel de classe 5). Utilitaire disponible et téléchargeable gratuitement sur le site intégrateur de l'ASIP Santé : http://integrateurs-cps.asipsante.fr/
2	Une fois votre certificat de chiffrement récupéré, l'importer (avec sa clé privée) dans le magasin personnel des certificats Microsoft en double-cliquant sur le fichier p12 récupéré.
3	Mettre à disposition le certificat (partie publique du bi-clé de confidentialité) auprès de ses interlocuteurs

7.4.2 Configurer Microsoft Outlook pour déchiffrer des emails

Cette procédure explique les manipulations à réaliser pour **déchiffrer** et **signer** numériquement des messages à partir des certificats de chiffrement délivrés par l'ASIP Santé.

#	Déchiffrer des messages à partir des certificats de chiffrement délivrés par l'ASIP Santé.
1	Menu "Outils" => "Centre de gestion de confidentialité" => "sécurité de messagerie électronique" => "Paramètres" => "Nouveau".
2	Saisir un nom de paramètre de sécurité (par exemple « Sécurité CPS »)
3	Bouton « Choisir » (certificat de chiffrement) => sélectionner le certificat de chiffrement généré à l'aide de CleoCPS et de la carte CPS du porteur (Certificat « Classe-5 »)
4	Choisir « 3DES » pour l'algorithme de chiffrement

NB : Ce paramétrage peut s'ajouter au paramétrage de signature d'email décrit plus haut.

7.5 Chiffrement de messages électroniques

Cette procédure explique les manipulations à réaliser pour **chiffrer** numériquement des messages à partir des certificats de chiffrement délivrés par l'ASIP Santé.

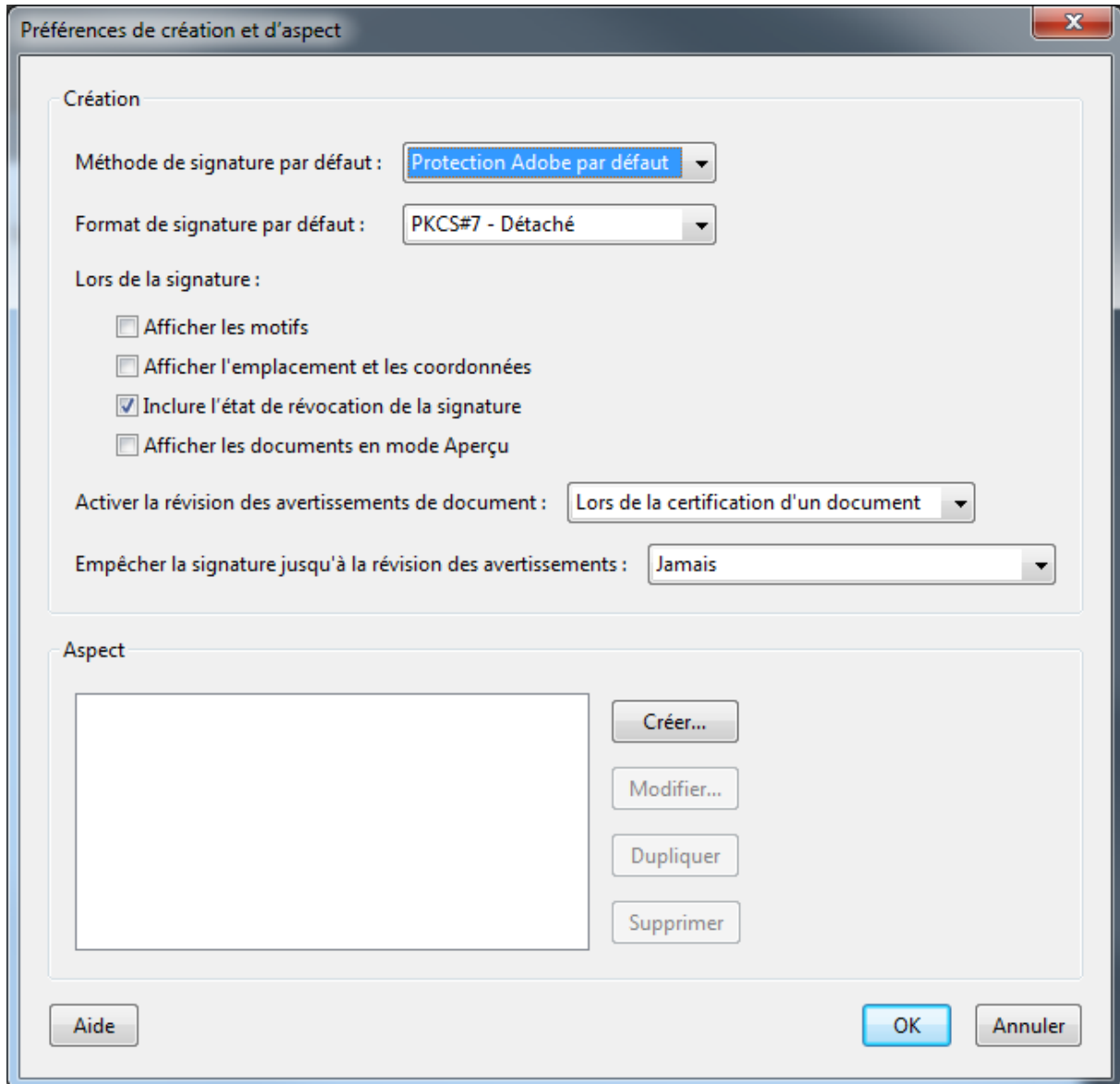
#	Chiffrer des messages à partir des certificats de chiffrement des contacts.
1	Associer votre correspondant à sa clé publique (certificat de chiffrement) dans Outlook : Avant d'envoyer un message chiffré à votre correspondant, il faut tout d'abord récupérer son certificat de chiffrement puis l'associer à son compte Outlook.
2	Pour récupérer le certificat de votre correspondant, plusieurs possibilités : Si le correspondant possède un certificat Classe 5 de confidentialité : se connecter à l'annuaire de l'ASIP Santé et récupérer son certificat de chiffrement (http://annuaire.gip-cps.fr/) Le correspondant envoie directement son certificat de chiffrement (format .cer ou .p7c) ou sa carte de contact (avec le certificat intégré) A la réception d'un message signé de votre correspondant, ajouter celui-ci à vos contacts (son certificat sera présent, si celui-ci est intégré à son message) Ce certificat peut être directement configuré depuis le serveur Microsoft Exchange par votre administrateur de messagerie, dans ce cas, il n'y a rien à faire (les certificats de chiffrement seront déjà associés aux contacts).
3	Intégrer ce certificat de chiffrement au contact dans votre messagerie : Ouvrir le contact : menu « atteindre » => « contacts » => sélectionner ou créer un nouveau contact. Onglet « certificats » => « importer » => sélectionner le certificat de chiffrement de ce contact.
4	La messagerie est maintenant configurée pour chiffrer des e-mails (à la création d'un nouvel e-mail, cocher la case « chiffrer » dans la barre de menu, pour chiffrer votre message)

Remarque : Il est tout à fait possible de signer et chiffrer un même message.

8 Adobe Acrobat Reader

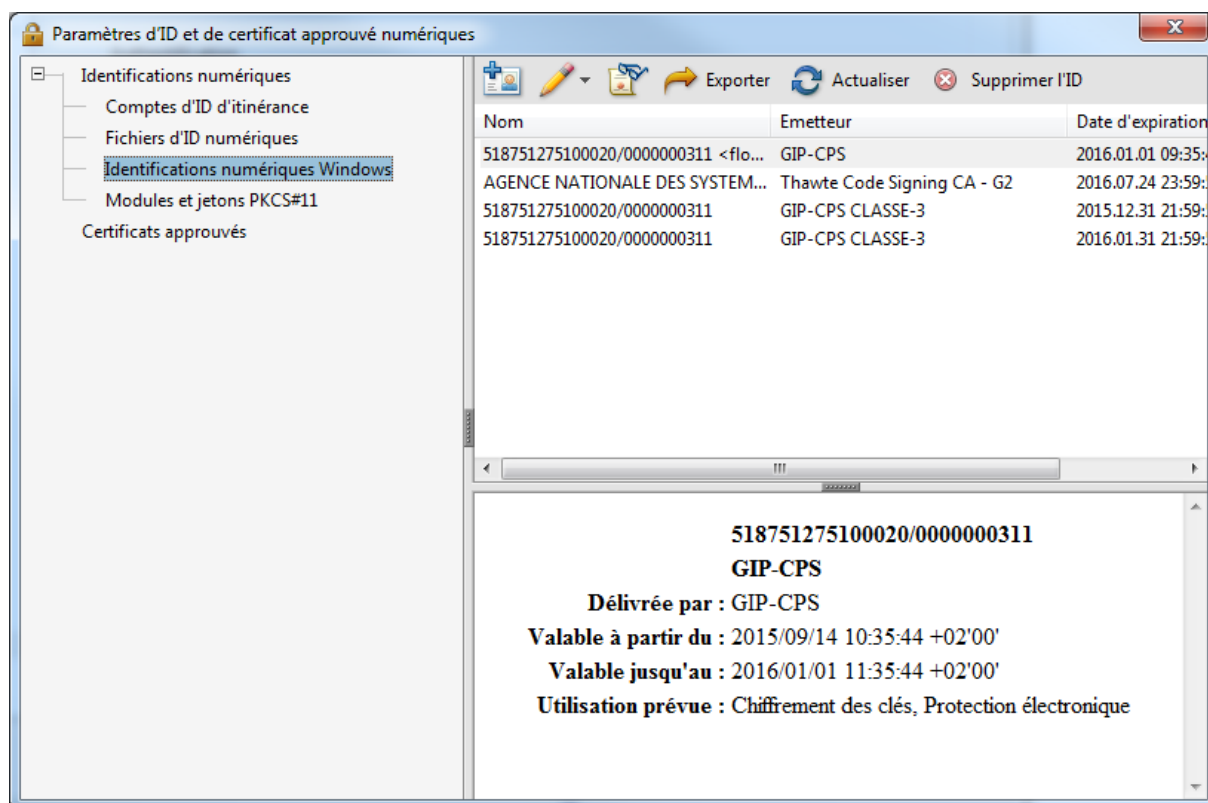
8.1 Signature de PDF avec Adobe Acrobat Reader

PDF supporte les formats de signature PKCS#7 détaché et:

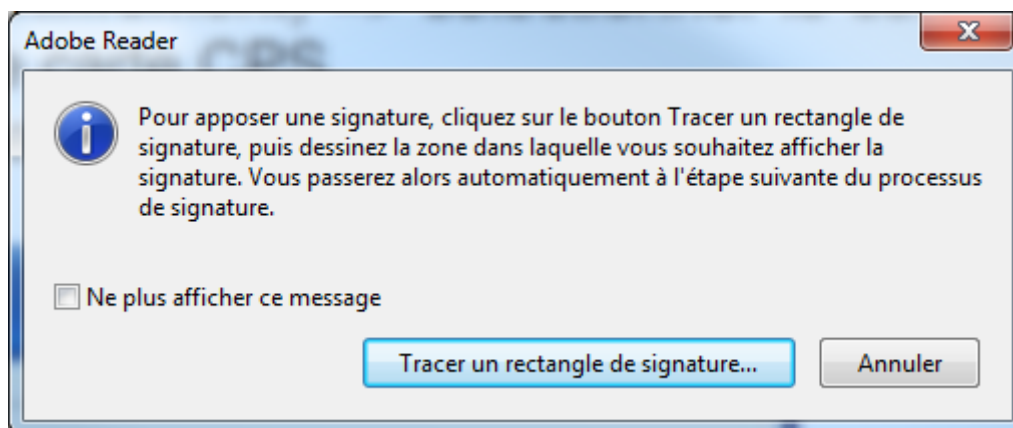


La section « Aspect » > « Créer » permet de changer l'aspect de la signature embarquée dans le document.

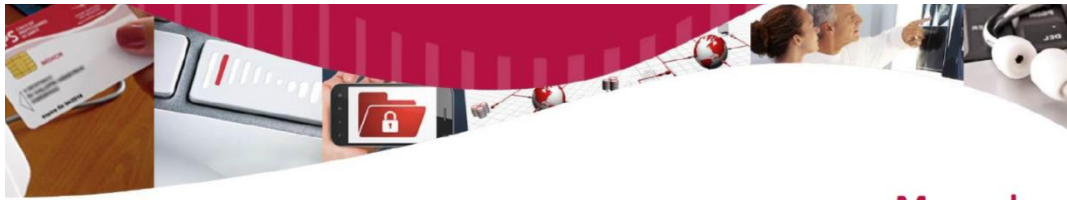
Une fois la Cryptolib CPS v5 installée, les certificats CPS sont directement vu par Acrobat (« Edition > Préférences > Signatures > Identités et certificats approuvés > Autres ») :



Il suffit dès lors d'ouvrir le PDF à signer et de sélectionner « Remplir et signer > Utiliser des certificats > Signer avec un certificat ». La fenêtre suivante apparaît :



« Tracer un rectangle de signature... », sélectionner une zone libre dans le document :



Manuel
d'installation et
d'utilisation
de la
Cryptolib CPS

Relâcher la souris, la fenêtre suivante apparaît :

Signer le document

Signature : 518751275100020/0000000311 (GIP-CPS CLASSE-3) 2016.01.31 ?

Emetteur du certificat : GIP-CPS CLASSE-3 Infos...

Aspect : Texte standard

51875127510
0020/000000
0311

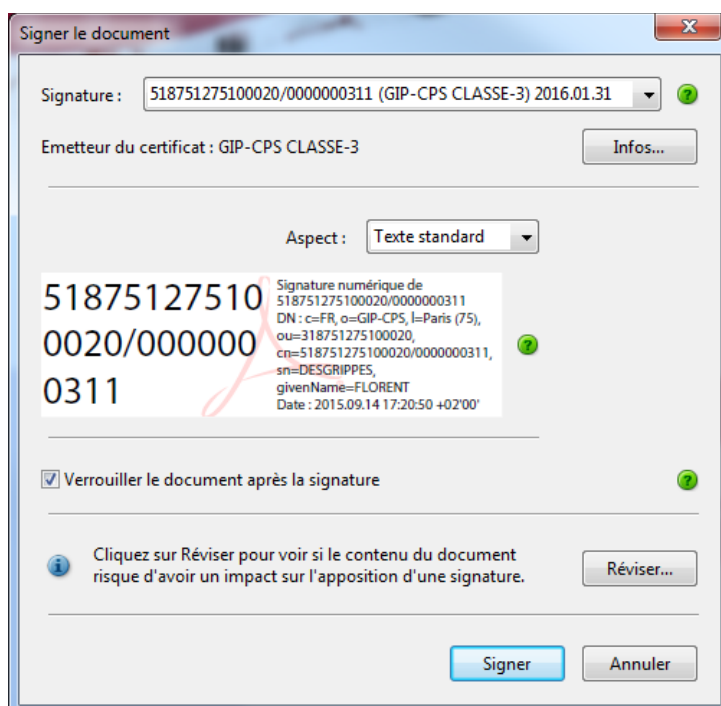
Signature numérique de
518751275100020/0000000311
DN : c=FR, o=GIP-CPS, l=Paris (75),
ou=318751275100020,
cn=518751275100020/0000000311,
sn=DESGRIPES,
givenName=FLORENT
Date : 2015.09.14 17:17:24 +02'00' ?

☐ Verrouiller le document après la signature ?

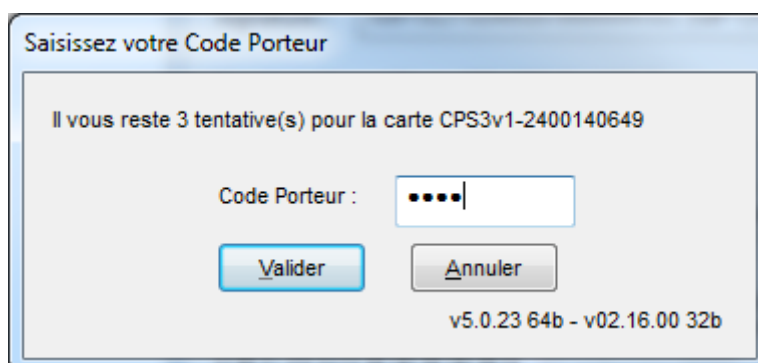
Cliquez sur Réviser pour voir si le contenu du document
risque d'avoir un impact sur l'apposition d'une signature. Réviser...

Signer Annuler

Choisir le certificat de signature et cocher « Verrouiller le document après la signature » :



« Signer », attendre, choisir un emplacement pour le fichier signé, entrer le code porteur :



8.2 Vérification de signature avec Adobe Acrobat Reader

8.2.1 Configuration

Il est nécessaire de configurer Adobe Acrobat Reader pour qu'il fasse confiance aux autorités de certification ASIP Santé. Pour cela, 2 options :

- 1- Lancer Adobe Acrobat Reader et assurer le paramétrage suivant :

« Edition > Préférences > Signatures > Authentification > Autres > Intégration à Windows > Approuver TOUS les certificats racine situés dans le magasin de certificat Windows pour : Validation de documents certifiés »

La clé de registre associée à ce dernier paramétrage est :

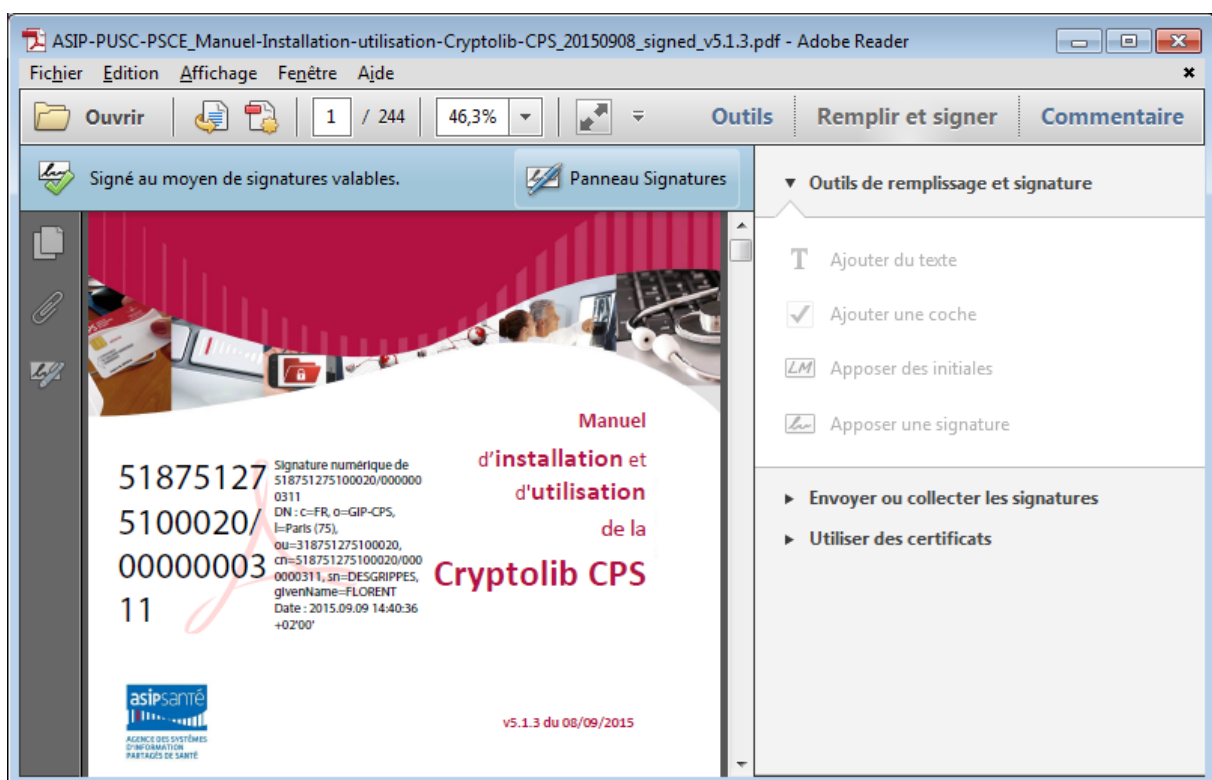
HKCU\Software\Adobe\Acrobat Reader\11.0\Security\CASPKI\cMSCAPI_DirectoryProvider\iMSStoreTrusted (DWORD) avec la valeur: 0x62

- 2- Insérer les certificats racines et intermédiaires de l'ASIP Santé dans le magasin de certificats Adobe Acrobat Reader explicitement :

« Edition > Préférences > Signatures > Identités et certificats approuvés > Autres > Certificats approuvés » > Insérer les certificats ASIP Santé

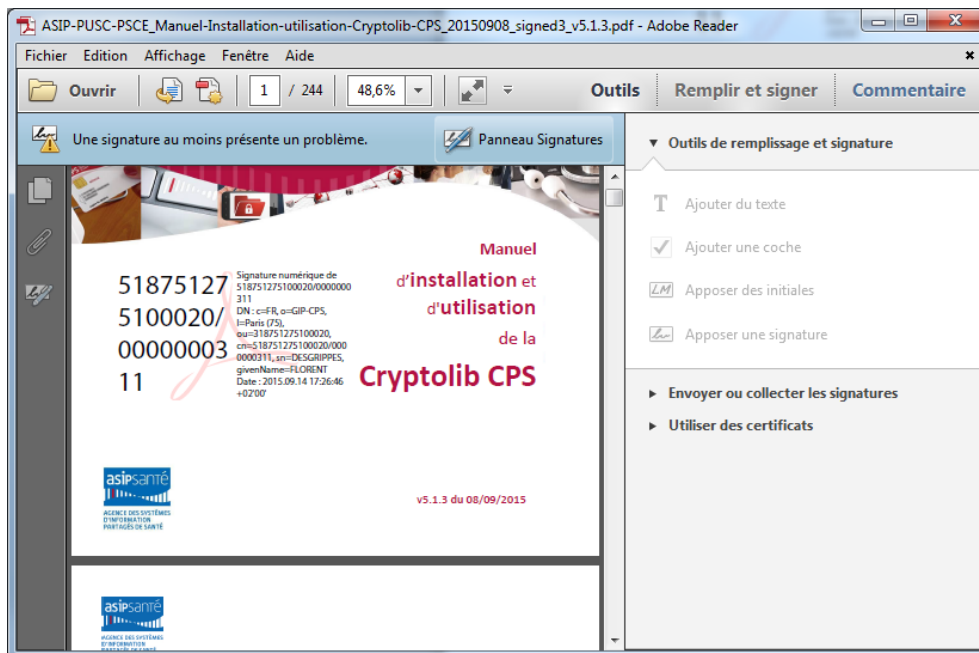
8.2.2 Vérification de signature

Ouvrir un PDF signé :

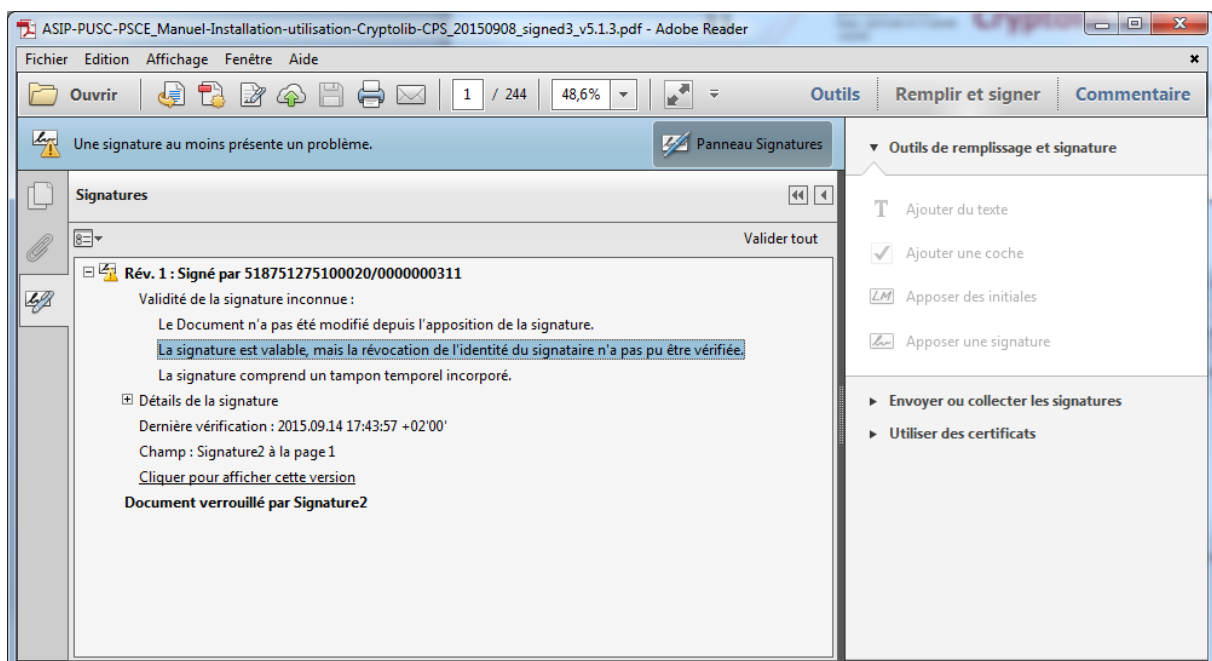


Le détail de la signature est disponible en cliquant sur le « Panneau Signatures ».

Adobe Acrobat Reader vérifie le statut du certificat de signature en contactant le domaine « annuaire.asipsante.fr ». Si ce domaine n'est pas résolu, l'erreur suivante apparaît :



« Panneau Signatures » :

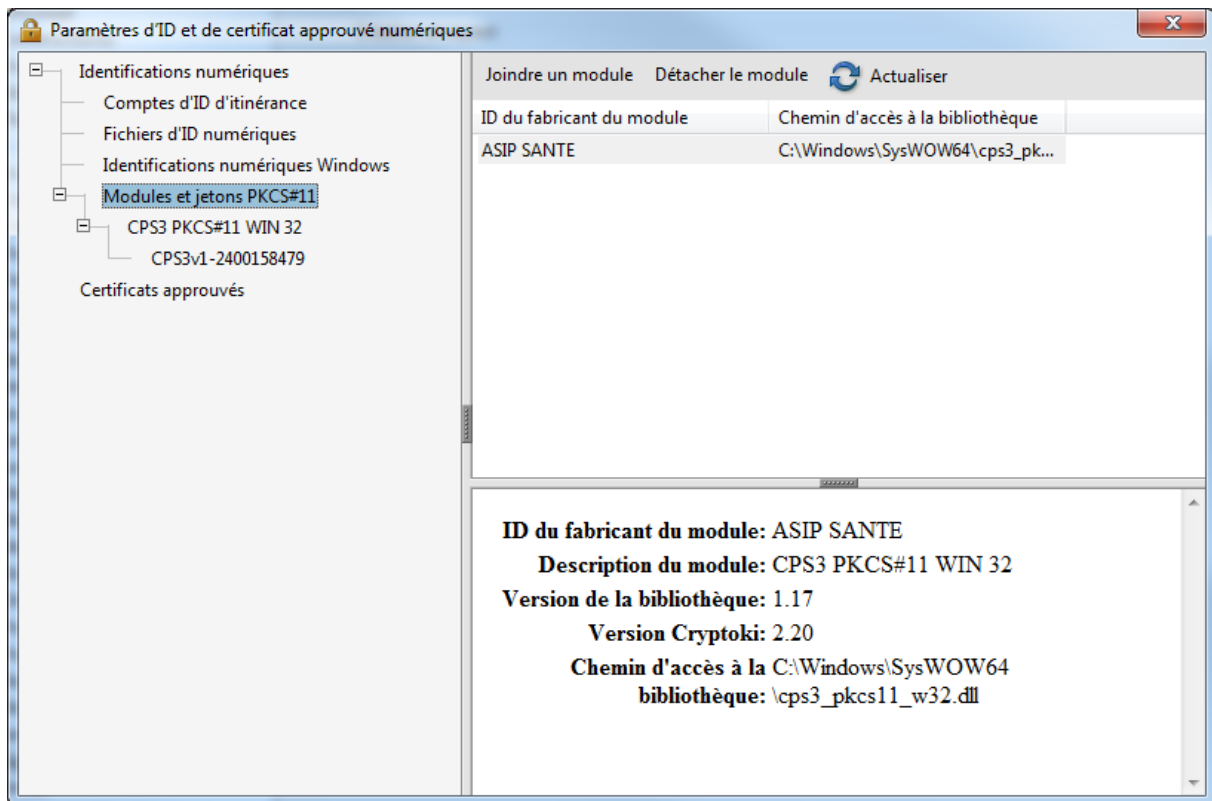


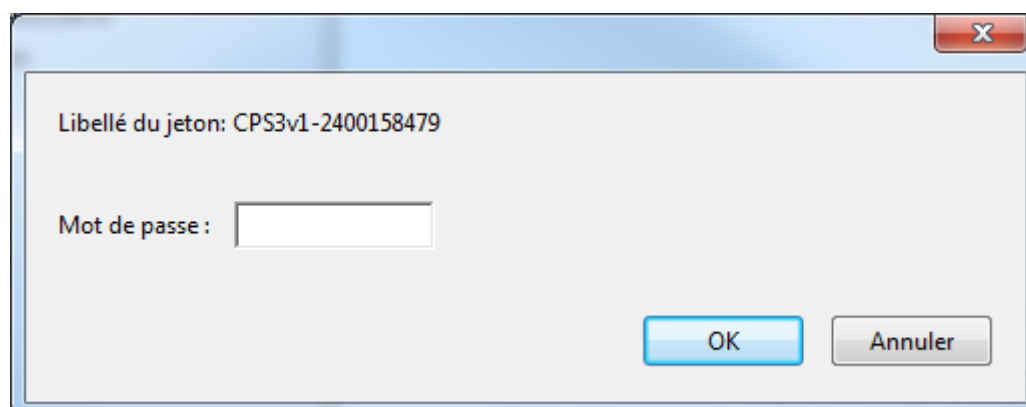
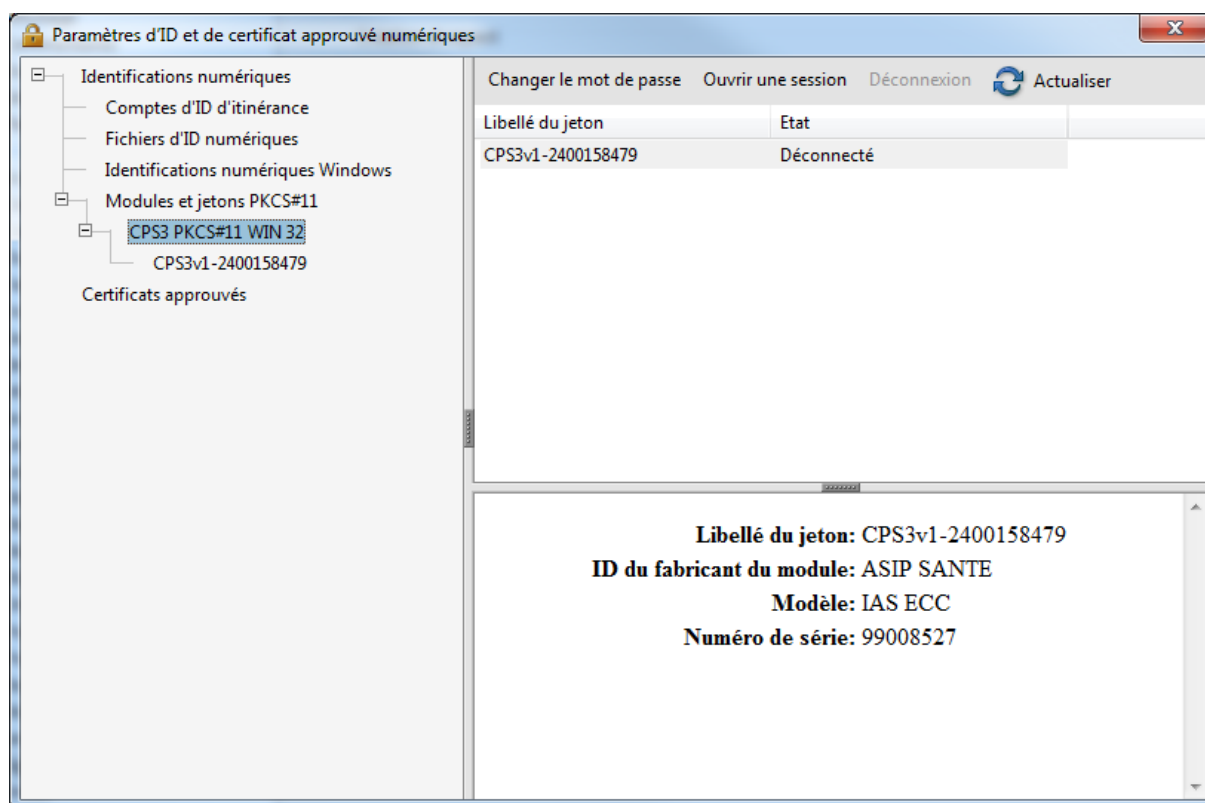
Noter que Adobe Acrobat Reader n'a pas besoin du PRAM pour vérifier le statut de révocation du certificat de signature employé.

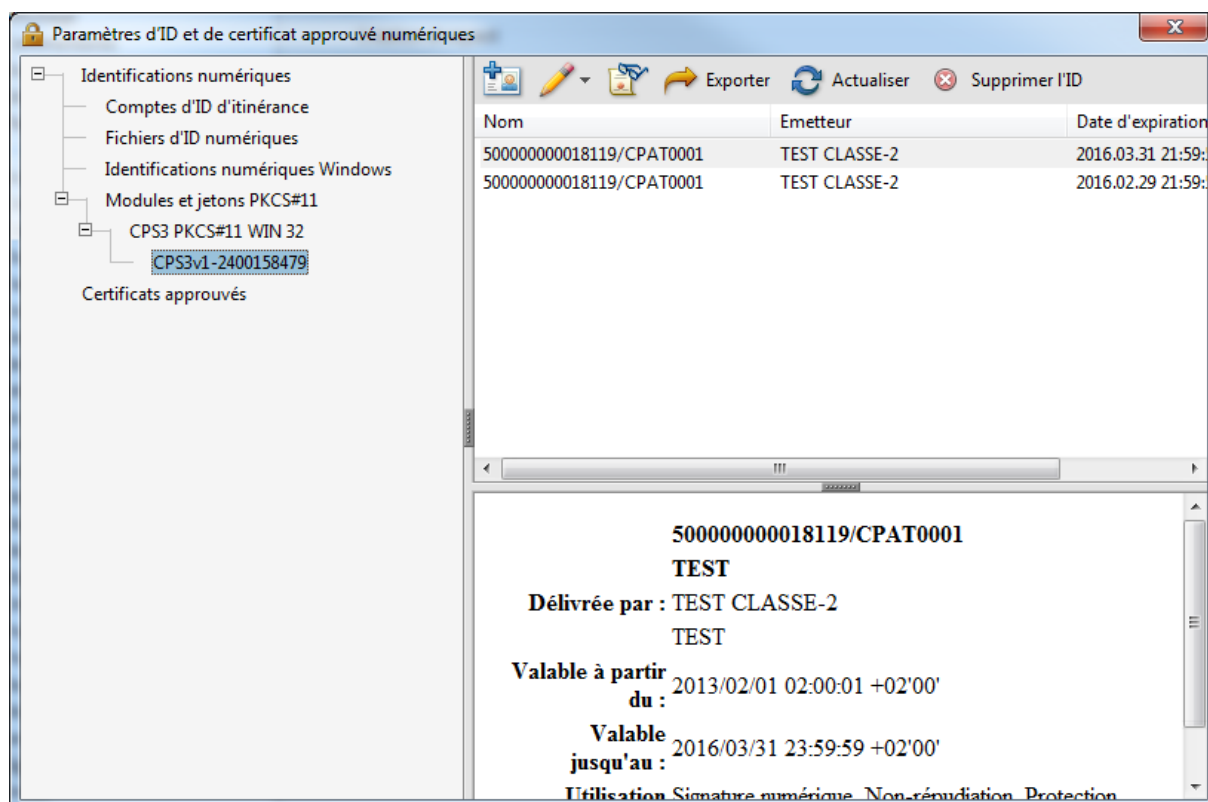
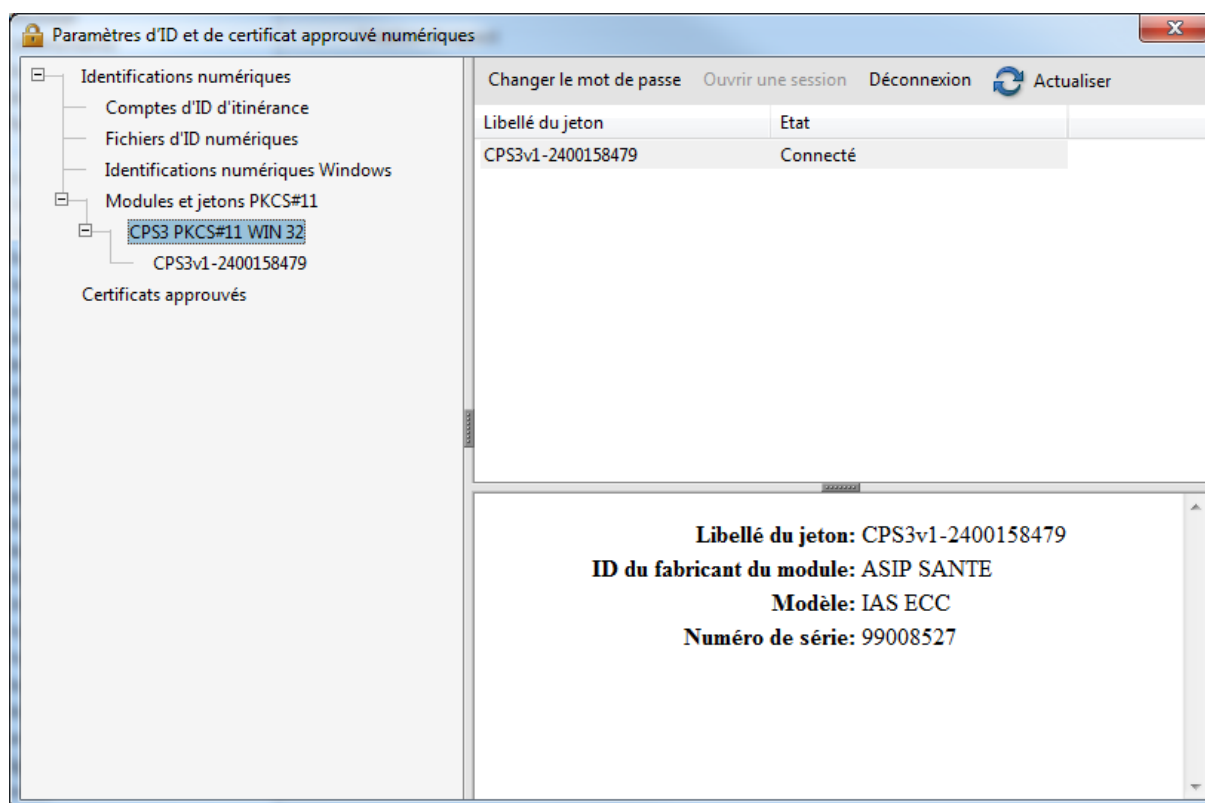
8.3 Utilisation du PKCS#11

Sous Windows sans CSP ou sous Mac OS X, il est aussi possible d'interfacer Adobe Acrobat Reader avec la CPS via le PKCS#11 :

« Edition > Préférences > Signatures > Identités et certificats approuvés > Autres > Modules et jetons PKCS#11 » :







8.4 Déploiement de Adobe Acrobat Reader en entreprise

Adobe a prévu des outils de personnalisation des installations de Adobe Acrobat Reader et des GPOs pour son produit :

<http://blogs.adobe.com/acrolaw/2013/02/acrobat-xi-deployment-guide-for-large-firms/>

<http://www.adobe.com/devnet-docs/acrobatetk/tools/AdminGuide/index.html>

<http://www.adobe.com/devnet-docs/acrobatetk/tools/AdminGuide/gpo.html>

Ce dernier lien pointe vers les ADM (liens FTP en haut de la page).

8.5 Création automatisée de documents PDF signés

Adobe distribue des API de création de documents PDF (« LiveCycle ES2 for Java developers » par exemple).

Ces APIs prévoient l'intégration d'une signature

<http://tv.adobe.com/watch/adobe-evangelists-duane-nickull/add-a-signature-field-to-a-pdf-using-the-java-api/>

http://help.adobe.com/en_US/livecycle/10.0/ProgramLC/javadoc/com/adobe/livecycle/signatures/client/SignatureServiceClientInterface.html

9 Conseils et Performances

9.1 Commande de produits de certification



Adéquation besoin et commande de produits de certification

La nouvelle IGC de Santé (PFCNG) permet de passer commande de nombreux produits de certification (certificats logiciels de personnes physiques, d'organisations, de serveurs, de cartes). Chaque produit est destiné à un usage particulier. Il convient donc de formaliser les besoins et d'identifier les produits de certification qui les couvrent, par exemple en commandant des produits qui contiennent des adresses mail si on souhaite faire de la signature d'email avec Outlook (S/MIME ou signature avec extension RFC822).

Tableau 10 : Adéquation besoin et commande de produits de certification

9.2 Provider de révocation ASIP Santé / Microsoft (PRAM)



Mises en œuvre sous Windows

Les mises en œuvre de mécanisme de sécurisation (signature, confidentialité) sous Windows nécessitent souvent l'installation et la configuration du PRAM. Toutes les informations et le téléchargement de ce module se trouve à l'adresse suivante : <http://www.microsoft.com/france/interop/ressources/gip-cps.aspx>

Tableau 11 : Mise en œuvre sous Windows et PRAM



Mises en œuvre sous Windows

Le PRAM ne sera plus nécessaire avec la nouvelle IGC de Santé (PFCNG).

Tableau 12 : PRAM et PFCNG

9.3 Récupération des CRLs ASIP Santé

L'outil qui signe et l'outil qui vérifie la signature doivent pouvoir résoudre le nom de domaine « annuaire.asipsante.fr » afin de télécharger les CRLs ASIP Santé.

Dans tous les cas, il faut s'assurer que les CRLs ASIP Santé sont obtenues par chaque poste en contactant « annuaire.asipsante.fr » mais en recevant les CRLs depuis le cache d'un « reverse-proxy cache » mis en œuvre sur le LAN faute de quoi :

- Les vérifications de statuts de révocation seront longues
- La charge sur les serveurs de CRLs ASIP sera très importante

9.4 Sécurisation de mails « point à point » versus MSSanté



MSSanté

Les préconisations de l'ASIP Santé concernant la sécurisation de messageries électroniques se sont recentrées vers la MSSanté, notamment du fait des difficultés de mise en œuvre que l'on perçoit sur ce sujet plus haut dans le document (commandes de certificats, distribution de certificats, associations {certificats ; contacts} dans un annuaire, spécificité de vérifications des statuts de certificats, charges de télé-chargements de CRLs sur les serveurs...)

Tableau 13 : MSSanté

9.5 Calcul du Hash

La signature peut être longue du fait du hashage préalable à la signature effective par la carte.



Calcul du Hash de la donnée à signer par la Cryptolib CPS v5

Le calcul du hash de la donnée à signer doit être effectué par la Cryptolib CPS v5 pour assurer une signature IAS via par exemple cps3_pkcs11_w32.dll ou cps3_pkcs11_w64.dll (cf. Manuel d'installation et d'utilisation de la Cryptolib CPS v5).

Tableau 14 : Calcul du Hash de la donnée à signer par la Cryptolib CPS v5

10Annexe – Liste des figures

Figure 1 : Architecture d'accès à la CPS avec Outlook en configuration PC/SC	9
Figure 2 : Architecture d'accès à la CPS avec Outlook en configuration PSS	10

11Annexe – Liste des tableaux

Tableau 1 : Références	3
Tableau 2 : contact accompagnement ASIP Santé	3
Tableau 3 : Glossaire	5
Tableau 4 : Entreprises citées.....	6
Tableau 5 : Avertissements	7
Tableau 6 : Prérequis.....	8
Tableau 7 : Clé Security absente	11
Tableau 8 : Signature CPS avec Outlook et PFCNG	11
Tableau 9 : Redémarrage d'Outlook	11
Tableau 10 : Adéquation besoin et commande de produits de certification	30
Tableau 11 : Mise en œuvre sous Windows et PRAM	30
Tableau 12 : PRAM et PFCNG	30
Tableau 13 : MSSanté.....	31
Tableau 14 : Calcul du Hash de la donnée à signer par la Cryptolib CPS v5.....	31

12Notes

[fin du document]



Agence des systèmes d'information partagés de santé
9, rue Georges Pitard - 75015 Paris
Tel : 01 58 45 32 50
esante.gouv.fr